Safeguard Computer Security Evaluation Matrix (SCSEM)

CA-ACF2

Release IV

10-Dec-07

Tester: *Insert Tester Name*
Date: *Insert Date(s) Testing Occured*
Location: *Insert Location testing was conducted*
Agency POC(s): *Insert Agency interviewee(s) names*

Test ID	NIST ID (800-53/A)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments/Supporting Evidence
1	AC-3,AU-2, AU-3, SAMG-05	The use of powerful programs and utilities is routinely logged.	Procedures: Review the “LOGGED PROGRAMS” (LOGPGM record) section of the CA-ACF2 Control Options (GSO Record). Although access rules and other options (e.g. GSO Control Options such as (a) (b) and (c) specified above) control the use of these programs, the LOGPGM record provides a facility to produce audit trails that log all datasets accessed by any of these programs. Determine if the use of programs specified under the following GSO Control Options are logged accordingly:	Expected Results: (a) “Restricted Program Names” (b) “Maintenance Logonids/Programs/Libraries” (c) “Tape Bypass Label Processing/Libraries”			
2	AC-3,AU-2, AU-3, SAMG-05	Ensure programs and users that bypass tape label verification will be logged.	Procedures: Review the TAPE BLP setting under “OPTIONS IN EFFECT” section of ACF2 GSO Control Options. TAPE BLP denotes whether or not an audit log is generated when programs or users bypass tape label processing.	Expected Results: LOG			
3	AU-2, AU-3, SAMG-05	ACF2 security records are properly recorded in SMF audit logs.	Procedures: Review the ACF2 COMMON setting under “SYSTEM PARAMETERS IN EFFECT”; “SMF RECORD NUMBERS” section of ACF2 GSO Control Options. ACF2 COMMON denotes the record number specified in the SMF log key for ACF2 functions.	Expected Results: 230, or the appropriate ACF2/SMF value specified in SYS1.PARMLIB (SMFPRMxx) member.			
4	AC-6, IA-2	Ensure ACF2 verifies access requests initiated by any system / started tasks.	Procedures: Review the STC OPTION setting under “OPTIONS IN EFFECT” section of ACF2 GSO Control Options. STC OPTION denotes whether or not a system/started task must be authenticated by ACF2 before access to any dataset is permitted.	Expected Results: -ON (STC OPTION=OFF denotes that ACF2 will not authenticate access request initiated by a system/started task, regardless of the access rules established for the specific system resource.)			
5	IA-2	Ensure logonids submitting batch jobs are authenticated through designation of the JOB attribute.	Procedures: Review the JOB CHECK setting under “OPTIONS IN EFFECT” section of ACF2 GSO Control Options. (JOB CHECK denotes whether or not logonids submitting batch jobs are authenticated through designation of the JOB attribute)	Expected Results: -YES			

6	IA-2	Ensure access violations, accumulated by user batch jobs submitted to the system, are restricted.	Procedures: Review the MAX VIO PER JOB setting under “OPTIONS IN EFFECT” section of ACF2 GSO Control Options. (MAX VIO PER JOB denotes the maximum number of access violations a batch job is permitted to accumulate before ACF2 terminates the job session.)	Expected Results: 3			
7	AC-5, AC-6	Determine if ACF2 is used for TSO user logon validation	Procedures: Review the UADS setting under “OPTIONS IN EFFECT” section of ACF2 GSO Control Options. (UADS denotes whether or not the User Attribute Dataset (UADS) is used for TSO logon procedures; UADS=BYPASS denotes that UADS dataset is bypassed and TSO logons are authenticated by CA-ACF2 through active TSO fields defined in each CA-ACF2 logonid record; UADS=USE denotes that user TSO sessions are authenticated through SYS1.UADS. If UADS is used, review procedures for the control and maintenance of the UADS dataset (SYS1.UADS).)	Expected Results: -BYPASS			
8	AC-7, PMG-10	Terminal sessions are cancelled after three (3) unsuccessful password attempts.	Procedures: Review the LOGON RETRY COUNT setting under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options. (LOGON RETRY COUNT denotes the maximum number of unsuccessful password attempts allowed before a terminal session is cancelled.)	Expected Results: 3			
9	IA-2, PMG-16	Passwords are required for all logonids (except for STC and RESTRICT).	Procedures: Review the PSWD REQUIRED setting under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options.	Expected Results: -YES			
10	IA-3, PMG-04	Users are permitted to change their passwords.	Procedures: Review the PSWD ALTER setting under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options.	Expected Results: -YES			
11	AC-7, PMG-10	Password violations accumulated by batch jobs are counted toward the MAX-PSWD ATTEMPTS.	Procedures: Review the PSWD-JES setting under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options.	Expected Results: -ON			
12	IA-3, PMG-09	Password expiration warning is 5-14 days before the password change interval (MAXDAYS) is enforced.	Procedures: Review the PSWD WARN DAYS setting under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options.	Expected Results: 5-14 days			

13	IA-3, PMG-01	Minimum password length is eight (8) characters.	Procedures: Review the MIN PSWD LENGTH setting under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options. (MIN PSWD LENGTH denotes the minimum number of characters required for establishing a user password.)	Expected Results: 8			
14	IA-3, PMG-17	Passwords are prohibited from being equivalent to a user’s logonid.	Procedures: Review the PSWD-LID setting under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options.	Expected Results: -YES			
15	IA-2, PMG-01, PMG-17	Passwords must contain alphanumeric characters, with a minimum of one (1) numeric character or (1) special charater.	Procedures: Review the following settings under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options.	Expected Results: -PSWDNMIC [forces at least 1 numeric] -PSWDALPH [forces at least one alpha]			
16	IA-2, PMG-06	Password history prohibits the reuse of passwords for six generations.	Procedures: Review the following settings under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options.	Expected Results: -PSWDHIST [forces password history of 4] -PSWXHIST [forces extended password history] -PSWXHIST#(2) [specifies number of extra stored - 4+2=6]			
17	IA-2, PMG-17	Passwords are prohibited from being composed of all numeric characters.	Procedures: Review the PSWD NUMERIC setting under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options.	Expected Results: -YES			
18	IA-2, PMG-17	Passwords are prohibited from containing repeating characters.	Procedures: Review the PSWDPAIR setting under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options.	Expected Results: -PSWDPAIR(0)			
19	IA-2, PMG-01, PMG-16, PMG-17	Reserved words are utilized to enforce password complexity.	Procedures: Review the PSWD RESERVE WORD setting under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options.	Expected Results: Common acronyms, prefixes, software system names, abbreviations, company names, etc. should be listed here.			
20	IA-3, PMG-04	Users are forced to change passwords at next logon whenever someone other than the user changes the user’s password.	Procedures: Review the PSWD FORCE setting under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options	Expected Results: -YES			

21	AC-7, PMG-10	User logonids are disabled after three (3) unsuccessful password attempts.	Procedures: Review the MAX PSWD ATTEMPTS setting under “PASSWORD OPTIONS IN EFFECT” section of ACF2 GSO Control Options. (MAX PSWD ATTEMPTS denotes the maximum number of unsuccessful password attempts allowed before a user’s logonid is suspended/disabled.)	Expected Results: 3			
22	IA-3, PMG-02, PMG-03	Password change interval “MAXDAYS” is appropriately set between 30-90 days.	Procedure: Obtain a user logonid (LID) report for general users and for a selected group of privileged users (e.g. Security Administrators, MVS Programmers/Support, Data Center Operations). Review the value specified MAXDAYS field associated with the aforementioned logonids selected. (MAXDAYS denotes the number of days allowed between password changes before the password expires.)	Expected Results: 90 - For standard users 60 - For privileged users			
23	IA-3, PMG-07	Users are prohibited from changing their passwords for at least 15 days after a recent change. Meaning, the minimum password age limit shall be 15 days after a recent password change.	Procedure: Obtain a user logonid (LID) report for general users and for a selected group of privileged users (e.g. Security Administrators, MVS Programmers/Support, Data Center Operations). Review the value specified MINDAYS field associated with the aforementioned logonids selected. (MINDAYS denotes the number of days required between password changes.)	Expected Results: 15			
24	AC-2, IA-3, PMG-05	Inactive accounts are revoked/suspended after 90 days of inactivity.	Procedure: 1. Obtain the ACF2 Super List Report for all logonids defined to the installation. Review the right hand most column that is a date field. Identify all logonids with date of last access exceeding 90 days from date of the review. 2. Verify that the logonids are revoked (i.e., ensure SUSPEND or CANCEL fields are specified in the logonid record) after a period of inactivity has expired. 3. Determine if policies and procedures are established to revoke inactive logonids after a specified period (e.g. 30, 60, or 90 days) has elapsed.	Expected Results: CANCEL or SUSPEND field values are specified in logonids with the “Date of Last Access” field exceeding 90 days from the date of the security review.			

25	CM-3	Network Job Entry (NJE) I & A security options are active.	Procedures: Review the “NJE OPTIONS IN EFFECT” section of ACF2 GSO Control Options. Through inquiry and observation, determine if site uses NJE. If NJE is not used, evaluation of NJE Option settings is not required.	Expected Results: VALIDATE INCOMING JOBS (IN) = YES VALIDATE OUTGOING JOBS (OUT) = YES INHERITANCE ALLOWED (IN) = YES SEND ENCRYPTED PASSWORD (OUT) = YES DEFAULT LOGONID = NONE			
26	IA-2	ACF2 displays the date and time of the user’s last system access whenever the user logs on to the system	Procedures: Review the NOTIFY setting under “SYSTEM PARAMETERS IN EFFECT”; “OTHER” section of ACF2 GSO Control Options. (NOTIFY denotes whether or not information displayed about the user’s last login date and time will verify that unauthorized user of their logonid has not occurred since the user’s last authentic logon session.)	Expected Results: -YES			
27	AC-10	User logons are terminated if wait time exceeds two (2) minutes	Procedures: Review the LOGON WAIT TIME setting under “SYSTEM PARAMETERS IN EFFECT”; “TSO RELATED DEFAULTS ACTIVE” section of ACF2 GSO Control Options. (LOGON WAIT TIME denotes the number of seconds used by ACF2 to time user responses and to subsequently abort the logon if the wait time parameter is exceeded. Settings exceeding 120 seconds should be evaluated for appropriateness.)	Expected Results: 60-120 seconds.			
28	IA-6, PMG-14	Clear-text representation of passwords shall be suppressed (blotted out) when entered at the login screen.	Procedures: Review the TSOTWX and TSO2741 settings in the TSO section of ACF2 GSO Control Options. These settings define a cross-out mask to obliterate the password on TWX and 2741 devices respectively.	Expected Results: TSOTWX: CR(15) IDLE(17) LENGTH(8) M1(X) M2(N) M3(Z) M4(M) STRING() TSO2741: BS(16) LENGTH(8) M1(X) M2(N) M3(Z) M4(M) STRING()			
29	PMG-18	Users shall commit passwords to memory, avoid writing passwords down and never disclose passwords to others (e.g., with a co-worker in order to share files).	Procedures: Interview the IAM. Verify that policies and training are in place to ensure that users protect passwords appropriately. If possible, walk through the office areas and ensure that passwords are not written down (e.g. look for sticky-notes, passwords taped to keyboard bottoms, etc.)	Policies and training are in place to ensure that users protect passwords appropriately.			
30	PMG-15	Passwords shall not be automated through function keys, scripts or other methods where passwords may be stored on the system.	Procedures: Interview the IAM. Verify that policies and training are in place to ensure that users understand that passwords will not be automated or stored in clear text on the system.	Policies and training are in place to ensure that users understand that passwords will not be automated or stored in clear text on the system.			

31	PMG-12	Default vendor passwords shall be changed upon successful installation of the information system product.	Procedures: Interview the SA and IAM. Verify that procedures are in place requiring that default passwords for installed products are changed as part of the installation process.	Default passwords for installed products are changed as part of the installation process.			
32	SM-2	Ensure firmware and hardware components of the system are routinely reviewed using internal diagnostic software.	Procedures: Obtain understanding of the OS platform environment and review procedures used to perform routine diagnostic checks and maintenance on the system firmware and hardware components.	Firmware and hardware components of the system are routinely reviewed using internal diagnostic software			
33	AC-3, AC-14	Programs that can bypass system security are maintained on the “RESTRICTED PROGRAM NAMES”.	Procedures: Review the “RESTRICTED PROGRAM NAMES” section of the CA-ACF2 Control Options (GSO Record).	Expected Results: Ensure the following sensitive programs are listed: (1) IEHINIT**** (2) FDR*** (3) DRWD**** (4) ICKDSF** (5) IEHD**** (6) *MASPZAP (7) DITTO			Note: Programs that should be maintained as “RESTRICTED PROGRAMS NAMES” (PPGM record) are those programs that do not initiate standard system services (e.g. open SVCs). Consequently, these programs can circumvent ACF2 / SAF intercept points and compromise system security. Placing the aforementioned programs on the “RESTRICTED PROGRAM NAMES” list restricts the use and delegation of such programs to users with the PPGM, NON-CNCL, or unscoped SECURITY attribute. Note: Programs specified in PPGM should be stored in CA-ACF2-protected libraries (e.g. *MASPZAP is stored in SYS1.MIGLIB) to prohibit unauthorized users from (a) reading and copying these programs into unsecured libraries; and (b) executing the copied programs under an uncontrolled name (i.e., not included on PPGM list).

34	SM-2	Entries included on "MAINTENANCE LOGONIDS/PROGRAMS/LIBRARIES" are restricted to the minimum programs required to perform DASD maintenance or other related operations.	Procedures: Review the "MAINTENANCE LOGONIDS/PROGRAMS/ LIBRARIES" (MAINT record) section of the CA-ACF2 Control Options (GSO Record).	Expected Results: Verify with appropriate systems personnel that: - All entries in the table are used for DASD maintenance or other related functions. - All program entries in the table are (1) exclusively maintained in ACF2-protected libraries, and (2) are accessible by authorized logonid(s) to perform activities commensurate with the existing user job function (e.g. DASD management)***. - All program entries are included in the "LOGGED PROGRAMS" section of the CA-ACF2 Control Options (GSO Record).			Note: The logonids specified in these program entries are required to have the NON-CNCL or the MAINT attribute to ensure proper program execution. Consequently, these logonids allow users to execute these programs and circumvent explicit access rules (i.e., dataset authorization checking) and logging/auditing facilities specified for libraries that store these programs. Therefore, to mitigate the risk of unauthorized activities occurring without detection, the aforementioned entries should be specified under the "LOGGED PROGRAMS" section of the ACF2 Control Options (GSO Record).
35	AC-6	Programs and libraries specified in "TAPE BYPASS LABEL PROGRAMS/LIBRARIES" are authorized and approved by appropriate system personnel, as needed, to bypass tape-label verification in order to perform inherent job functions.	Procedures: Review the "TAPE BYPASS LABEL PROGRAMS/LIBRARIES" (BLPPGM Record) section of the CA-ACF2 Control Options (GSO Record).	Expected Results: Interview appropriate system personnel and evaluate the justification for authorizing tape BLP capabilities for all programs specified.			Note: The GSO BLPPGM record grants a program the authority to use tape bypass label processing (BLP). This option is enforced at the program level – whether or not BLP authority is provided to users. In addition, the BLPLOG field, specified as "TAPE BLP" section of CA-ACF2 GSO Control Options, logs all uses of BLP (i.e., TAPE BLP = LOG) – either by (a) a program authorized in the GSO BLPPGM record; or (b) a user authorized through the TAPE-BLP or TAPE-LBL attribute specified on the user's logonid record.

36	CM-3	To determine if MODE is set to ABORT	Procedures: Review the MODE setting specified in the CA-ACF2 Control Options (GSO Record). MODE=ABORT denotes ACF2 denies access to a dataset unless explicitly defined/permitted by the dataset access rule. All access violations are logged. MODE= LOG denotes ACF2 permits all access attempts to datasets, regardless of the dataset access rules. All access violations are logged. MODE=QUIET denotes ACF2 permits all access attempts to datasets, regardless of the dataset access rules. However, access violations are not logged. MODE=WARN denotes ACF2 permits all access attempts to datasets, regardless of the dataset access rules. All access violations are logged and an access-violation message is sent to user's terminal. MODE=RULE is deemed a selective mode, where conditional actions can be executed if the existing access rule does not permit the user's request to access to dataset.	Expected Results: -ABORT			
37	AC-6	Access rule sets are sorted in the order of most specific to most general.	Procedures: Review the NOSORT setting under "OPTIONS IN EFFECT" section of ACF2 GSO Control Options. (NOSORT=NO denotes that access rule sets are sorted in order of most specific rules to most general rules. This ensures rule entries are executed in sequence specified in the rule set.)	Expected Results: -NO			Note: If NOSORT=YES and a $NOSORT statement is specified in an access rule set, ACF2 sorting of rules from most specific to most general is suppressed. Consequently, general rules placed before specific rules could inadvertently supersede the specific rules appearing later on in the access rule set. Therefore, a setting of YES should be justified by and discussed with the data owner or security administrator responsible for the rule set.

38	AC-6	Tape dataset protection is active/in effect	Procedures: Review the TAPE DSN setting under "OPTIONS IN EFFECT" section of ACF2 GSO Control Options. (TAPE DSN denotes whether or not tape dataset protection is enforced before granting access. Tape dataset protection is enforced only if (a) setting = YES; and (b) Tape Management System (e.g. CA-1, TLMS) is in use. If setting is NO, only tape datasets defined to SECVOLS will have their access rules enforced.)	Expected Results: -YES, or alternatively - Option DSNAME PROTECTED VOLUMES and VOLSER PROTECTED VOLUMES (note this is referencing SECVOL) contain the entry "******" and TAPE DSN = YES or NO.			To ensure optimal protection of tape and DASD datasets, RESVOLS, SECVOLS, and TAPE DSN configuration should be evaluated collaboratively to determine the residual or collective impact of dataset protection enforced by CA-ACF2 access rules.
39	AC-6	DASD datasets/volumes are protected through list specified by RESVOLS.	Procedures: Review the – DSNAME PROTECTED VOLUMES -- setting under "RULES/DIRECTORY RESIDENCY OPTIONS" section of ACF2 GSO Control Options.	Expected Results: Since RESVOLS, SECVOLS, and TAPE DSN configurations function collaboratively to protect DASD and tape volumes, the following configurations provide adequate protection: (1) Optimal Solution = RESVOLS "******", SECVOLS has no masking compositions or naming patterns defined, and TAPE DSN = YES. (2) RESVOLS and SECVOLS = "******" and TAPE DSN = YES or NO. (3) RESVOLS = "******", SECVOLS with any setting, and TAPE DSN = YES.			
40	AC-6	DASD volumes and/or tape volumes are protected through list specified by SECVOLS.	Procedures: Review the – VOLSER PROTECTED VOLUMES -- setting under "RULES/DIRECTORY RESIDENCY OPTIONS" section of ACF2 GSO Control Options.	Expected Results: Since RESVOLS, SECVOLS, and TAPE DSN configurations function collaboratively to protect DASD and tape volumes, the following configurations should provide adequate protection: (1) Optimal Solution: RESVOLS "******", SECVOLS has no masking compositions or naming patterns defined, and TAPE DSN = YES. (2) Alternative: RESVOLS and SECVOLS = "******" and TAPE DSN = YES or NO. (3) Alternative: RESVOLS = "******", SECVOLS with any setting, and TAPE DSN = YES.			

41	AC-6	Decompile authorities are restricted to logonids with SECURITY or AUDIT attributes.	Procedures: Review the DECOMP AUTHORITY setting under “RULES/DIRECTORY RESIDENCY OPTIONS” section of ACF2 GSO Control Options. (DECOMP AUTHORITY denotes the types of users authorized to decompile (but not alter) and display access/resource rules regardless of restrictions placed by scope records.)	Expected Results: SECURITY or AUDIT.			
42	AC-6	Listing Infostorage records are restricted to logonids with SECURITY or AUDIT attributes.	Procedures: Review the INFO LIST AUTH setting under “RULES/DIRECTORY RESIDENCY OPTIONS” section of ACF2 GSO Control Options. (INFO LIST AUTHORITY denotes the logonid attributes authorized to display the records (e.g. GSO records, resource rules, scope records, entry records) stored in the Infostorage database. Also, scoped users can list all Infostorage database records, except for resource rules.)	Expected Results: SECURITY or AUDIT.			
43	AC-6	UID string modifications are restricted to logonids with SECURITY or AUDIT attributes.	Procedures: Review the UID setting under “RULES/DIRECTORY RESIDENCY OPTIONS” section of ACF2 GSO Control Options. (UID denotes a string of concatenated fields that controls the definition of each user’s UID record. The string composition is derived from the existing Field Definition Record (FDR). Each field should be reviewed to determine which users can alter (ALTER=) specific fields in the string - - thereby potentially altering access authorities granted to users.)	Expected Results: Consequently, UID string alterations should be restricted to users with unscoped SECURITY or AUDIT attributes. Furthermore, the RESTRICT attribute should be used in conjunction with SECURITY or AUDIT with each of the field definitions specified in the UID string. SECURITY or AUDIT.***			

44	CM-3	Users are prohibited from entering their username and password on the same line.	Procedures: Review the QUICK LOGON setting under "SYSTEM PARAMETERS IN EFFECT"; "TSO RELATED DEFAULTS ACTIVE" section of ACF2 GSO Control Options. (QUICK LOGON denotes whether or not users can enter their passwords and logonids on the same line. YES indicates the password value will not be masked and will be displayed in plain text when entered.)	Expected Results: -NO			
45	AC-6	ACF2 intercepts received control	Procedures: Review the "ACF2 INTERCEPTS THAT HAVE RECEIVED CONTROL". Evaluate the appropriateness for each intercept that has not received control as specified by the (NO) setting.	Expected Results: At a minimum, the following ACF2 intercepts should receive control: DASD-ALLOC (YES) JOB INIT (YES) DASD-OPEN (YES) PROGRAM-CALL (YES) TSO-MVS (YES)			
46	AC-6	MVS System Authorization Facility (SAF) calls are controlled by ACF2 security.	Procedures: Review the "SYSTEM AUTHORIZATION FACILITY DEFINITIONS" and verify that the SUBSYS parameter is "ACF2". If not, evaluate the feasibility or potential security implications of SAF calls / request not specified under the default ACF2 process (i.e., installation defined).	SUBSYS parameter is "ACF2"			
47	AC-6	The SECURITY and ACCOUNT privileges are adequately controlled.	Procedures: Using the LIST IF command or the SL report, document who has the SECURITY or the ACCOUNT privilege. Inquire of appropriate personnel the justification for each user assigned these privileges. -SECURITY attribute allows: (1) access all datasets, protected programs and resources; (2) maintain all records in the Infostorage database; and (3) change and display logonid records. -ACCOUNT- The ACCOUNT attribute permits users to insert, catalog, and delete logonids (unless restricted or "scoped" by the SCPLST logonid field). Users with the ACCOUNT attribute only, cannot catalog or change logonid records for users with both the ACCOUNT and SECURITY attributes.	Expected Results: SECURITY and ACCOUNT privileges have been granted to a limited number of users with a security responsibility.			

48	AC-6	The NON-CNCL privileges are adequately controlled.	Procedures: Using the LIST IF command or the SL report, determine who has the NON-CNCL privilege. Inquire of appropriate personnel the justification for each user or login ID assigned this privilege. The NON-CNCL attribute specifies ACF2 cannot terminate or “cancel” a user’s request to access a dataset to which the user is not explicitly authorized through an access rule set. However, ACF2 logs all uses of NON-CNCL authority.	Expected Results: No more than 3 or 4 such users should be found, and these should be used for emergency purposes (e.g. started task IDs, assigned to FIRECALL IDs) only. In addition, their usage should be reviewed.			
49	AC-6	The READALL privileges are adequately controlled.	Procedures: Using the LIST IF command or the SL report, determine who has the READALL privilege. Inquire of appropriate personnel the justification for each user or Login ID assigned this privilege. (READALL grants the user the authority to open any file for READ and EXEC regardless of the rules and only applies to datasets.)	Expected Results: The READALL privilege should be limited to security Started Tasks and Emergency logonids.			
50	AC-6	The AUDIT privilege is adequately controlled.	Procedures: Using the LIST IF command or the SL report, determine who has the AUDIT privilege. Inquire of appropriate personnel the justification for each user or Login ID assigned this privilege. (AUDIT grants the user the authority to display logonid records, access rules, resource rules, and Infostorage records (e.g. GSO record), and all ACF2 system control options.)	Expected Results: The AUDIT privilege should be restricted to security auditors and/or security administrators			
51	AC-6	The MAINT privileges are adequately controlled.	Procedures: Using the LIST IF command or the SL report, determine who has the MAINT privilege. Inquire of appropriate personnel the justification for each user or Login ID assigned this privilege. (MAINT grants the user the authority to execute any program defined in the MAINT GSO; “MAINTENANCE LOGINIDS/PROGRAMS/LIBRARIES”. Without logging or access rule verification.)	Expected Results: Only maintenance jobs having a business need to manage/maintain the logonids, programs, or libraries listed in the MAINT GSO section should be assigned this privilege.			

52	AC-6	The TAPE BLP privileges are adequately controlled.	Procedures: Using the LIST IF command or the SL report, determine who has the TAPE-BLP privilege. Inquire of appropriate personnel the justification for each user or Login ID assigned this privilege. (The TAPE-BLP attribute permits users to bypass label processing (BLP) when accessing tape datasets.)	Expected Results: Limited access should be granted to this privilege and restricted to personnel routinely tasked with performing tape management job functions.			
53	AC-6	The ALLCMDS privileges are adequately controlled.	Procedures: Using the LIST IF command or the SL report, determine who has the ALLCMDS privilege. Inquire of appropriate personnel the justification for each user or Login ID assigned this privilege. (The ALLCMDS attribute permits users to circumvent the ACF2 restricted command list.)	Expected Results: Limited access should be granted to this privilege and restricted to personnel routinely tasked with performing job functions requiring use of ALLCMDS privilege. Evaluate delegation of this privilege for reasonableness.			
54	AC-6	The REFRESH privileges are adequately controlled.	Procedures: Using the LIST IF command or the SL report, determine who has the REFRESH privilege. Inquire of appropriate personnel the justification for each user or Login ID assigned this privilege. (The REFRESH attribute permits users to issue the ACF2 REFRESH operator command from the operator console. Consequently, users can apply dynamic changes to records (e.g., GSO record) maintained in the Infostorage database.)	Expected Results: Limited access should be granted to this privilege and should be restricted users (e.g., security administrators) routinely tasked with applying changes to records (e.g. GSO record) maintained in the Infostorage database.			
55	AC-6	The RULE_VLD privileges are included in the Security Administrators LID Record.	Procedures: LIST each logonid record that has the SECURITY privilege and verify that the RULEVLD attribute is present. (The RULEVLD attribute denotes all user access (in particular, access by data owners and users with the SECURITY attribute) to datasets and resources must be explicitly permitted by the access rules established for the dataset or resource.)	Expected Results: The RULEVLD attribute should be included in the logonid record for logonids with the SECURITY attribute.			

56	AC-8	The system shows a IRS-approved screen-warning banner that outlines the consequences /penalties for misusing the system.	Procedures: Review warning banner online to ensure compliance with IRS requirements.	Expected Results: The warning banner is compliant with IRS guidelines. The warning banner should indicate users are subject to monitoring and are subject to penalties and prosecution. Sample Warning Banner Text is as follows: *UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both. All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials.*			

57	AC-6	Access to ACF2 distribution libraries are controlled.	Procedures: 1. Obtain the Access Rules (report) from the security officer for for ACF2 distribution libraries (generally denoted by the high level prefix CAI.*) 2. The ACF2 distribution libraries contain the load modules for the ACF2 software product. Examples of ACF2 load modules include the ISPF (Interactive System Productivity Facility) interface panels, macros, or vendor-developed JCL (Job Control Language) procedures. 3. Through inquiry of the security officer, determine the name and job function of each user listed separately or within a Group on the Access Control List. Determine whether users having access is appropriate and based on a need to know, least privilege concept. Only systems programmers tasked with routinely maintaining the ACF2 system product should have ALLOCATE authority to these datasets.	Only systems programmers tasked with routinely maintaining the ACF2 system product have ALLOCATE authority to these datasets.			
58	AC-6	FTI datasets are restricted to users having a “need to know”.	Procedures: 1. Obtain the Access Rules (report) from the security officer for each FTI dataset. Note: The applications programmer or production control group may have to assist in identifying all FTI datasets. 2. Through inquiry of appropriate personnel, (data security, programming, data center operations) determine the name and job function of each user listed separately or within a group on the access control list. Determine whether users having access is appropriate and based on need to know and the least privilege concept. Given the nature of these datasets, even READ access maybe inappropriate. Note: Data Security, Systems and Application Programmers, Data Center Operations, and Production Control typically do not need to have routine access to these datasets. FIRECALL or EMERGENCY IDs are the preferred control to grant temporary access to FTI datasets.	Users have access as appropriate and based on need to know and the least privilege concept. FIRECALL or EMERGENCY IDs are the control used to grant temporary access to FTI datasets.			

59	AU-2, AU-3, SAMG-04	Audit trails are generated for READ and above access attempts to FTI data sets.	Procedures: 1. Request the System Administrator to generate an ACF2 data set access report for FTI data sets. 2. Review the report and verify that access to the FTI data sets is properly logged, and is restricted to authorized personnel. Using the previously obtained list of users authorized to access FTI data sets, verify that: a. Users logged as accessing FTI data sets are on the list of authorized users; b. No accesses to FTI data sets are logged for users not on the list; c. Logging records include READ accesses, as well as Write/Allocate accesses.	Access to FTI data sets is properly logged.			
60	AC-6	ALLOCATE (ALLOC) authority to core MVS operating system libraries are restricted to MVS programmers.	Procedures: Obtain the Access Rules (report) from the security officer for each of the critical SYS1 datasets: -SYS1.PROCLIB -SYS1.LINKLIB -SYS1.LPALIB -SYS1.MIGLIB -SYS1.PARMLIB -SYS1.SVCLIB -SYS1.UADS -SYS1.VTAMLIB -SYS1.VTAMLST -SYS1.NUCLEUS Through inquiry of the security officer, determine the name and job function of each user listed separately or within a Group on the Access Control List. Determine whether users having ALLOC authority have a need for this level of access.	Expected Results: Only systems programmers should have ALLOC authority to these datasets.			

61	AC-6	Logical access to ACF2 databases is properly restricted.	Procedures: Obtain the Access Rules (report) from the security officer for each ACF2 security database (including backups) using the high level prefix: SYS1.ACF* or applicable high-level prefixes for the following datasets/libraries: -SYS1.ACF2.RULES -SYS1.ACF2.LOGINIGS -SYS1.ACF2.INFOSTG -SYS1.ACF.BKLIDS -SYS1.ACF.BKRULES -SYS1.ACF.BKINFO Through inquiry of the security officer, determine the name and job function of each user listed separately or within a Group on the Access Control List.	Expected Results: NO users should have ALLOC or WRITE access to these databases. (Note: Access to these databases can be granted via emergency purposes using a FIRECALL or EMERGENCY ID).			
62	AC-3	System exits specified on the system are authorized, approved and appropriate.	Procedures: Review the " -- LOCAL EXITS SPECIFIED ON THIS SYSTEM ---" section of the ACF SHOW ACTIVE report. For exits not = NONE, inquire of appropriate systems personnel as to (a) the purpose of the system exit (b) the business justification for the system exit (c) the system users responsible for maintaining the system exit (d) how ACF2 administers security to control logical access to the system exit code.	Procedures: All exits are properly justified and documented.			Note: Due to inherent weaknesses in ACF2 password security controls, some installations may deploy (with installation-specific configurations) the NEW PSWD VALIDATE exit routine to enforce a more granular level of password controls, such as enforcing alphanumeric password composition requirements and enhancing password-history parameter controls.
63	CM-3, SC-4	AUTOERAS feature is specified for FTI datasets and related volumes.	Procedures: Review the -- AUTOMATIC ERASE VOLUMES -- setting under "OPTIONS IN EFFECT" section of ACF2 GSO Control Options. (AUTOERAS denotes the type of datasets and volumes where physical erasure is performed during deletion (scratch).)	Expected Results: Volume name(s) specified for FTI datasets and/or a naming pattern/masking composition that represents FTI dataset name(s).			

64	SS-2	Agency maintains documentation for the Information System Component. The documentation is readily available, protected when required and distributed to authorized personnel.	Procedures: Review the Information System Component Documentation e.g. guides or manuals for privileged users (e.g., administrators, programmers, production control) and end-users on configuring, installing and operating the OS/System Software; and optimizing the system's security features to ensure compliance with the security objective.	Appropriate documentation is maintained.			
65	AC-11	The information system prevents further access to the system by initiating a session lock after [an organization-defined time period] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.	Confer with the IAM and SA. Verify that interactive sessions (TSO, TPX, etc.) are locked after a period of inactivity in accordance with IRS guidelines. The inactivity time should be 15 minutes or less.	Interactive sessions are locked after the requisite period of time.			
66	AC-12, SC-10	The information system automatically terminates a remote session after [an organization-defined time period] of inactivity. (1) Automatic session termination applies to local and remote sessions.	Confer with the IAM and SA. Verify that interactive sessions (TSO, TPX, SSH, etc.) are terminated after a period of inactivity in accordance with IRS guidelines.	Interactive sessions are terminated after the requisite period of time.			
67	AC-13, AU-6	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls. (1) The organization employs automated mechanisms to facilitate the review of user activities.	Confer with the IAM. Verify that procedures are in place to review audit logs on a regular, periodic basis, and that these procedure are followed (i.e. that the reviews are performed). Inquire whether automated data review and reductions tools are available and/or in use.	Audit logs are reviewed on a regular basis. Automated tools are used if available.			

68	AC-17	The organization authorizes, monitors, and controls all methods of remote access to the information system. (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. (3) The organization controls all remote accesses through a limited number of managed access control points. (4) The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	Confer with the IAM and SA. Determine how remote accesses are managed and controlled. If remote execution of privileged functions (administration, etc.) is permitted, ensure that such privileges are properly justified and documented. Ensure that remote sessions are properly encrypted.	Remote accesses are properly justified, documented, managed and controlled.			
69	AU-4	The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	With the systems programmer, review the size of the SYS1.MANx files, the %-utilization, and the schedule with whish the files are dumped (backed up) and cleared.	SYS1.MANx files are managed adequately to prevent the loss of system audit data.			
70	AU-5	The information system alerts appropriate organizational officials in the event of an audit processing failure	With the systems programmer, ensure that the system issues console alerts when the SYS1.MANx files approach critical threshold. Verify that the operations staff has standing instructions to notify the appropriate personnel, and that procedures have been established to dump the SMF data.	Appripriate console alerts are issued, and procedures exist to notify personnel and to manage the backup of SMF data.			
71	AU-7	The information system provides an audit reduction and report generation capability.	Confer with the IAM and the SA to determine what SMF data audit reduction and reporting tools are available (in addition to standard z/OS SMF reporting mechanisms.)	Data reduction tools are available and in use.			

72	AU-8	The information system provides time stamps for use in audit record generation. (1) The organization synchronizes internal information system clocks [Assignment: organization-defined frequency].	Confer with the Systems Programmer and IAM to determine the site policy and procedures for setting, verifying, and synchronizing the system clock. Inquire whether the system clock is set to GMT+0 with a Time Zone offset, or whether the system clock is set to local time.	Policy and procedures exist for setting and periodically synchronizing the system clock. Note: Audit data (SMF) time stamps should reflect GMT time.			
73	AU-9	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Determine in which library (SYS1.LINKLIB, etc.) the system audit data reporting tools reside. Obtain an access rules report for this library, and for SYS1.MAN*. Identify personnel who have access to the files and utilities. Ensure that no personnel have excessive access permissions.	Access to the SYS1.MANx filies and reporting tools is restricted to the appropriate personnel.			
74	AU-11	The organization retains audit records for [an organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Confer with the Systems Programmer and IAM to determine the site policy and procedures for dumping (backing up) SMF data and creating duplicate backups to prevent data loss. Determine that the site data retension policy is in accordance with IRS guidelines.	Policy and procedures exist for backing up and retaining SMF data.			
75	IA-4	The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [an organization-defined time period] of inactivity; and (vi) archiving user identifiers.	Confer with the IAM to deterimine the site policy and procedures for issuing, managing, revoking, and archiving user access credentials. Determine whether or not logon IDs are re-issued after they have been used.	The site should have adequate procedures in place to issue, manage, revoke, and archive user access credentials. User logon IDs should not be re-issued to new personnel once they have been used.			

76	IA-5	The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	Confer with the IAM to deterimine the site policy and procedures for issuing and disseminating initial user passwords, and for requiring and enforcing periodic system-wide password change.	The site should have adequate procedures in place for initial password dissemination and periodic system-wide password change.			
77	SC-2	The information system separates user functionality (including user interface services) from information system management functionality.	Interview the IAM and SA. Determine whether privileged users have separate accounts for performing day-to-day user activities than those used for performing privileged functions/tasks.	Privileged personnel should not use the same logon IDs for both normal and priveleged functions.			
78	SC-5	The information system protects against or limits the effects of denial of service attacks. (1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks. (2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.	Interview the IAM, SA, and Network Systems personnel. Determine what capabilities the system has to detect and prevent inbound and/or outbound flooding-based denial of service attacks	The system should provide protection against flood-type denial of service attacks.			
79	SC-23	The information system provides mechanisms to protect the authenticity of communications sessions.	Interview the IAM, SA, and Network Systems personnel. Determine what capabilities the system has to prevent network session hijacking	The system should provide protection against network session hijacking.			

80	SC-3, SC-8, SC-9, SC-13	FTI is encrypted while traversing networked, or interconnected systems from remote locations.	Procedures: Obtain a network diagram that depicts all access points used to process, store and transmit FTI – noting firewalls, routers, and switches where applicable. Determine if IP traffic (TN3270 terminal emulation sessions used to access application functions that process FTI, FTI file uploads/downloads) containing FTI is encrypted when traversing communication lines (e.g. T1, T3, ISDN) using encryption solutions including, but not limited to: Triple DES, SSL, TLS, or Secure IP Tunneling (VPN using IPSEC). Evaluate viable encryption alternatives for appropriateness.	IP traffic (TN3270 terminal emulation sessions used to access application functions that process FTI, FTI file uploads/downloads) containing FTI is encrypted when traversing communication lines (e.g. T1, T3, ISDN) using approved encryption solutions.			
81	SAMG-16/17	The audit trail shall be protected from unauthorized access, use, deletion or modification. The audit trail shall be restricted to personnel routinely responsible for performing security audit functions.	Procedures: 1. Request the System Administrator to generate an ACF2 data set access report. Review the report and verify that access to the SMF data sets (SYS1.MANx) is restricted to authorized personnel.	Access to the SMF data sets (SYS1.MANx) is restricted to authorized personnel.			
82	SAMG-1--15	Auditing is configured to capture security-relevant events.	Procedures: 1. Review SYS1.PARMLIB(SMFPRMxx) 2. Ensure that, at a minimum, all IBM (00-127), ACF2 (as defined in the ACFFDR, default 230), and TSOMON (199) SMF record types are written. Request documentation for any record types appearing in a NOTYPE(nn) parameter. 3. If SMF exits IEFU83, IEFU84, IEFU85 are listed, verify with the Systems Programmer the functions performed by the exits. Ensure that they do not suppress required SMF record types. 4. Verify that the system SMF data sets (SYS1.MANx) exist and are written to.	1. IBM (00-127), ACF2 (as defined in the ACFFDR, default 230), and TSOMON (199) SMF record types are written. . 2. Documentation exists for any record types appearing in a NOTYPE(nn) parameter. 3. If SMF exits IEFU83, IEFU84, IEFU85 are listed, they do not suppress required SMF record types. 4. The system SMF data sets (SYS1.MANx) exist and are written to.			
83	SAMG-1	The audit trail captures all successful login and logoff attempts.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 30, 32 ACF2: 230 (or as defined in ACFFDR)	The required data is collected.			

84	SAMG-2, SAMG-3	The audit trail captures all unsuccessful login and authorization attempts. The audit trail captures all identification and authentication attempts.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: ACF2: 230 (or as defined in ACFFDR)	The required data is collected.			
85	SAMG-5	The audit trail captures all actions, connections and requests performed by privileged functions	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 32	The required data is collected.			
86	SAMG-6	The audit trail captures all changes to logical access control authorities (e.g., rights, permissions).	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: ACF2: 230 (or as defined in ACFFDR)	The required data is collected.			
87	SAMG-7	The audit trail captures all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 90[-9], 90[-10] ACF2: 230 (or as defined in ACFFDR)	The required data is collected.			

88	SAMG-8	The audit trail captures the creation, modification and deletion of objects including files, directories and user accounts. Pub 1075 5.6.2 states, "Security-relevant events must enable the detection of unauthorized access to FTI data." The test case needs to identify where the FTI resides on the file system and ensure that access to that specific directory and FTI files contained within is audited.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 17, 18, 19, 59, 60, 62, 63, 64, 67, 68, 69, 83, 92 ACF2: 230 (or as defined in ACFFDR)	The required data is collected.			
89	SAMG-9	The audit trail captures the creation, modification and deletion of user accounts and group accounts.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: ACF2: 230 (or as defined in ACFFDR)	The required data is collected.			
90	SAMG-10	The audit trail captures the creation, modification and deletion of user account and group account privileges	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: ACF2: 230 (or as defined in ACFFDR)	The required data is collected.			
91	SAMG-11	The audit trail captures: i) the date of the system event; ii) the time of the system event; iii) the type of system event initiated; and iv) the user account, system account, service or process responsible for initiating the system event.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 90	The required data is collected.			

92	SAMG-12	The audit trail captures system startup and shutdown functions.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 0, 22[-1]	The required data is collected.			
93	SAMG-13	The audit trail captures modifications to administrator account(s) and administrator group account(s) including: i) escalation of user account privileges commensurate with administrator-equivalent account(s); and ii) adding or deleting users from the administrator group account(s).	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: ACF2: 230 (or as defined in ACFFDR)	The required data is collected.			
94	SAMG-14	The audit trail captures the enabling or disabling of audit report generation services.	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 23	The required data is collected.			
95	SAMG-15	The audit trail captures command line changes, batch file changes and queries made to the system (e.g., operating system, application, database).	Procedures: 1. Request the System Administrator to generate SMF audit and security (SMFDUMP) reports by batch. 2. Review the Report and verify that the required data are collected for SMF record types: IBM: 22, 32, 83, 101, 110 ACF2: 230 (or as defined in ACFFDR)	The required data is collected.			

IRS Safeguard SCSEM Legend

Test Case Tab: Execute the test cases and document the results to complete the IRS Safeguard Computer Security review. Reviewer is required to complete the following columns: Actual Results, Comments/Supporting Evidence.

Test ID	Identification number of SCSEM test case
NIST ID	NIST 800-53/PUB 1075 Control Identifier
Test Objective	Objective of test procedure.
Test Steps	Detailed test procedures to follow for test execution.
Expected Results	The expected outcome of the test step execution that would result in a Pass.
Actual Results	The actual outcome of the test step execution, i.e., the actual configuration setting observed.
Pass/Fail	Reviewer to indicate if the test case pass, failed or is not applicable.
Comments / Supporting Evidence	Reviewer to include any supporting evidence to confirm if the test case passed., failed on not applicable As evidence, provide the following information for the following assessment methods: 1. Interview - Name and title of the person providing information. Also provide the date when the information is provided. 2. Examination - Provide the name, title, and date of the document referenced as the evidence. Also provide section number where the pertinent information is resident within the document (if possible). Ensure all supporting evidence to verify the test case passed or failed. If the control is marked as NA, then provide appropriate justification as to why the control is considered NA.